



1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202.719.7000
FAX 202.719.7049

7925 JONES BRANCH DRIVE
McLEAN, VA 22102
PHONE 703.905.2800
FAX 703.905.2820

www.wileyrein.com

September 4, 2008

Nancy J. Victory
202.719.7344
nvictory@wileyrein.com

VIA ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Ex Parte Presentation*, WT Docket Nos. 96-86, 96-198, 99-87, 01-289, 01-309, 02-55, 04-356, 06-150, 06-169, 07-166, 07-195; PS Docket Nos. 06-229, 07-114, 07-287, 08-51; WC Docket Nos. 02-60, 04-36, 05-196, 06-63; CC Docket Nos. 92-105, 94-102; EB Docket Nos. 04-296, 06-119; AU Docket No. 07-157; CG Docket No. 03-123; ET Docket No. 04-295; RM-9332; RM-11376

Dear Ms. Dortch:

Pursuant to Section 1.1206 of the Commission's Rules, I hereby submit *Homeland Security and Communications: A Compendium of Federal Programs* in the above-referenced dockets. If you have any questions regarding this presentation, please contact the undersigned.

Respectfully submitted,

/s/ Nancy J. Victory

Nancy J. Victory



Homeland Security and Communications: A Compendium of Federal Programs

Prepared by:

**Nancy J. Victory
Catherine M. Hilke**

September 2008



Introduction

The importance of communications in meeting homeland security needs of the United States is recognized in a large number of wide ranging federal programs and initiatives. This updated survey attempts to capture and categorize legislation pending before Congress, programs administered by the U.S. Department of Homeland Security, the role of the U.S. Department of Justice, activities arising before the Federal Communications Commission, and efforts at other government agencies and departments. The attached matrices reflect a best efforts attempt to provide a simple and timely overview of these complex, interrelated, and dynamic efforts.

About the Authors

Nancy J. Victory

202.719.7344

nvictory@wileyrein.com

Ms. Victory is a partner in the Communications Practice and chair of the International Telecommunications Practice, where she advises a broad cross-section of the industry on the business implications of regulatory policy. Previously she served as Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration under President Bush. Ms. Victory served as the Chair of the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks. She received her J.D., *cum laude* from the Georgetown University Law Center.

Catherine M. Hilke

202.719.7418

chilke@wileyrein.com

Ms. Hilke is an associate in the Communications Practice, where she is engaged in a wide variety of regulatory issues affecting the wireless industry. She received her J.D., *magna cum laude* from the Columbus School of Law, The Catholic University of America.



Table of Contents

FEDERAL COMMUNICATIONS COMMISSION	1	U.S. DEPARTMENT OF HOMELAND SECURITY	32
Spectrum	1	Network Security and Reliability	32
Spectrum Efficiency	4	Priority Service	41
Emergency Alerting	6	Emergency Alerting	44
911 and Disability Access	8	Other	45
CALEA	10	U.S. DEPARTMENT OF JUSTICE	47
Katrina	11	Interoperability	47
Airplane Communications	12	U.S. DEPARTMENT OF COMMERCE	50
Miscellaneous	13	Interoperability	50
Bureaus/Committees	14	U.S. DEPARTMENT OF AGRICULTURE	53
U.S. CONGRESS	17	Interoperability	53
Spectrum	17	U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES	54
Interoperability	18	Interoperability	54
Homeland Security Communications Grants	20		
Cybersecurity and Critical Infrastructure	21		
Emergency Alerting	23		
Communications Surveillance	24		
E-911 and Citizen Emergency Communications	28		
Border & Port Security	31		



Federal Communications Commission

SPECTRUM			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
700 MHz WT Docket No. 06-150 CC Docket No. 94-102 WT Docket No. 01-309 WT Docket No. 06-169 PS Docket No. 06-229 WT Docket No. 96-86 WT Docket No. 07-166 FCC 07-132	<p>The 700 MHz Band is currently used for the broadcast of analog television signals. This spectrum will be returned to the FCC upon completion of the Digital Television Transition, scheduled for February 17, 2009. Under the Digital Television and Public Safety Act of 2005, Congress allocated 24 MHz of the 700 MHz Band for public safety communications (the rest will be auctioned for commercial uses). Half of this spectrum has been set aside for narrowband voice communications services that must be provided under rigid technical standards designed to promote interoperability. The other half will be designated for interoperable broadband communications.</p> <p>The FCC adopted the following requirements for the 700 MHz spectrum:</p> <p><i>Public Safety Spectrum.</i> The Commission awarded the 12 MHz of spectrum designated for broadband communications to a single Public Safety Broadband Licensee. This Public Safety Broadband Licensee will lease access to the spectrum and the deployed network to individual public safety entities. A state or local public safety entity may either (a) build its own broadband network that meets the requirements and specifications of the shared network with pre-approval from the Public Safety Broadband Licensee; or (b) seek a waiver to operate a wideband network that is not inconsistent with an area's broadband deployment plan.</p>	<p>These decisions make more dedicated spectrum available for public safety communications. The selection of a single licensee will ensure the interoperability of broadband public safety communications.</p> <p>Additional commercial 700 MHz services also may be a useful tool for public safety.</p>	<p>Order released August 10, 2007.</p> <p>On November 19, 2007, the Commission released an Order selecting the Public Safety Spectrum Trust Corporation as the single nationwide licensee for the public safety 700 MHz broadband spectrum allocation.</p> <p>The auction for the commercial 700 MHz band (Auction 73) ran from January 24, 2008 to March 18, 2008. Although the auction raised \$19.592 billion in revenue, more than any previous FCC auction, the "D Block" did not receive a bid that met its \$1.3 billion reserve price.</p> <p>On March 20, 2008, the Commission released an Order de-linking the D Block from the other blocks offered in the auction to enable the Commission to disclose the winning bidders and move forward with spectrum licensing.</p> <p>In response to an FCC request, the Office of Inspector General (OIG) investigated allegations that improper meetings discouraged D Block bidders. On April 25, 2008, the OIG issued an investigative report dispelling such allegations and concluding</p>



SPECTRUM			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
700 MHz (cont.) WT Docket No. 06-150 AU Docket No. 07-157 WT Docket No. 06-150 PS Docket No. 06-229 FCC 08-128	<i>Commercial Spectrum.</i> The Commission also established service rules for the commercial portions of the 700 MHz Band. Among other things, the FCC initially concluded that the winner of the 10 MHz “D Block” license will be required to negotiate a network sharing agreement with the Public Safety Broadband Licensee under which the D Block licensee would build a network that encompasses both the D Block and the Public Safety Broadband Licensee spectrum.		<p>that the lease payment agreement discussed at Cyren Call’s meetings with Frontline and Verizon was not the sole cause of the D Block’s failure to attract bidders at the reserve price.</p> <p>On May 14, 2008, the Commission released a Second FNPRM seeking public comment on how the Commission should proceed with the reauction and licensing of the D Block while maximizing the public safety and commercial benefits of a nationwide interoperable broadband network. Comments were due June 20, 2008; replies were due July 7, 2008.</p> <p>On July 30, 2008, expert panelists discussed public safety interoperable communications and the 700 MHz D Block Proceeding in a public FCC hearing in New York City.</p>



SPECTRUM			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Advanced Wireless Services WT Docket No. 07-195 WT Docket No. 04-356 Report No. AUC-06-66-F FCC 08-158	<p>In 2006, 104 entities won 1087 licenses to provide advanced wireless services (AWS), including third generation (3G) mobile broadband, in the 1.7 and 2.1 GHz bands (AWS-1). These systems are intended to provide access to a wide range of telecommunications services and other services that are specific to mobile users. The 1.7 GHz band is currently licensed to a variety of federal government entities. The 2.1 GHz band is currently licensed to private and commercial fixed microwave systems. Incumbent licensees in both bands must be relocated by AWS licensees prior to service initiation.</p> <p>The FCC has allocated the 1915-1920 MHz, 1995-2000 MHz, and 2155-2180 MHz bands for commercial Advanced Wireless Services (AWS-2).</p>	<p>NTIA worked with the Department of Defense and other federal agencies to develop a set of proposals to clear the 1.7/2.1 GHz bands for AWS.</p> <p>Commercial AWS services may be a useful tool for first responders.</p>	<p>AWS-1 licensees are currently in negotiations with federal government incumbents regarding relocation.</p> <p>In June 2008, the FCC released a Further Notice of Proposed Rulemaking seeking comment on proposed service rules for the AWS-2 bands. Comments were due July 25, 2008; replies were due August 11, 2008.</p>



SPECTRUM EFFICIENCY			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
800 MHz Rebanding WT Docket No. 02-55 FCC 04-168 FCC 04-294 DA 07-27 DA 07-1648 FCC 07-92 FCC 07-102 DA 08-1444 DA 08-1449	<p>Public safety and Commercial Mobile Radio Service (CMRS) providers operate in the 800 MHz band on adjacent frequencies. Due to technical incompatibilities, interference to public safety operations occurred. The FCC required Sprint Nextel to surrender some of its 800 MHz spectrum and fund the relocation of public safety and other incumbents to new frequency assignments in the 800 MHz band. In exchange, the FCC issued Sprint Nextel a license for 10 MHz of spectrum in the 1.9 GHz PCS band.</p> <p>The rebanding process is being implemented by an independent Transition Administrator (TA) comprised of BearingPoint, Squire Sanders Dempsey LLP and Baseline Telecom, Inc.</p> <p>Rebanding began on June 27, 2005 and was originally scheduled for completion by June 26, 2008.</p>	<p>Reconfiguration of the 800 MHz band is designed to decrease interference between public safety radio systems and commercial systems.</p>	<p>On September 12, 2007, the Commission issued a public notice outlining supplemental procedures and providing guidance for completion of 800 MHz rebanding by National Public Safety Planning Advisory Committee (NPSPAC) licensees.</p> <p>In 2007, the Commission issued an MO&O affirming that Sprint is required to vacate the Mid-Band by June 26, 2008. Sprint appealed the decision to the Court of Appeals for the D.C. Circuit. The Court upheld the Commission's decision on May 2, 2008.</p> <p>On May 9, 2008, the Commission released a reconfigured 800 MHz band plan for U.S.-Canada border regions.</p> <p>On June 17, 2008, the Commission granted numerous requests by public safety licensees for waiver of the June 26, 2008 deadline to complete 800 MHz rebanding.</p> <p>On June 19, 2008, the Commission issued an Order granting Sprint's request to temporarily remain on those channels (1-120) that will not be required by rebanding public safety licenses until after the June 26, 2008 deadline.</p> <p>In response to a Petition for Relief filed by Sprint, the Commission issued an Order on June 20 waiving the June 26, 2008 deadline for vacating the interleaved channels in the Mid-Band for a period of 30 days.</p>

SPECTRUM EFFICIENCY			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Transition to 6.25 kHz Narrowband Technology by PLMR Systems</p> <p>WT Docket No. 99-87</p> <p>RM-9332</p> <p>FCC 07-39</p> <p>FCC 04-292</p> <p>FCC 08-127</p>	<p>The FCC has established the following transition for requiring the use of more efficient technologies in certain land mobile frequency bands at 150-174 MHz and 421-512 MHz. The following deadlines are now in force:</p> <ul style="list-style-type: none"> On January 1, 2013, all private land mobile licensees (Business, Industrial and Public Safety) must operate with technology designed to operate within a 12.5 kHz channel. Broader bandwidth technologies are permitted provided that they offer equivalent efficiency. Applications for new or modified operations on 25 kHz channels will be accepted until January 1, 2011. After that date, applications specifying bandwidths greater than 12.5 kHz will be accepted only for equivalent efficiency designs. Manufacturers can continue to build and import equipment operating on channel bandwidths up to 25 kHz until January 1, 2011. After that date, the manufacture and importation of such equipment operating on a channel bandwidth greater than 12.5 kHz will be limited to equivalent efficiency designs. Beginning January 1, 2011, equipment certification applications must specify 6.25 kHz capabilities. 	<p>The “refarming” proceedings modified technical standards and operating conditions for public safety operations in the Public Safety Pool, allowing for the development of more advanced and efficient public safety services.</p>	<p>In March 2007, the FCC declined to establish a fixed date for private land mobile radio systems in the 150-174 MHz and 421-512 MHz bands to transition to 6.25 kHz narrowband technology, but strongly urged licensees to consider migrating directly to 6.25 kHz rather than first adopting 12.5 kHz technology and later migrating to 6.25 kHz technology. The Commission also required that certain equipment certification applications specify 6.25 kHz capabilities by January 1, 2011.</p> <p>On May 13, 2008, the Commission released an MO&O clarifying that a NPRM would be released prior to the adoption of a 6.25 kHz technology transition schedule. The Commission further explained that language encouraging licensees to consider migrating directly to 6.25 kHz technology was not intended to dissuade licensees that had already begun the process from migrating to 12.5 kHz technology.</p>

EMERGENCY ALERTING			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Next Generation Emergency Alert System Rulemaking</p> <p>EB Docket No. 04-296</p> <p>FCC 07-109</p>	<p>The Next Generation Emergency Alert System (Next Generation EAS) enables the President of the United States, state officials, and the National Weather Service to address the nation during an emergency by providing communications capability from broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, and direct broadcast satellite services.</p>	<p>The Next Generation EAS gives the government the ability to alert the public through a variety of media in case of an emergency or disaster.</p>	<p>In its July 12, 2007 Second R&O and FNPRM, the FCC required Next Generation EAS participants to accept text, audio, and video messages using the Common Alerting Protocol (CAP). It also sought comment on how to deliver warnings to persons with disabilities and non-English speakers, and how to ensure that the Next Generation EAS system will operate as intended.</p> <p>On August 13, 2007, the Public Safety and Homeland Security Bureau (PSHSB) released a letter reporting on stakeholder meetings regarding the provision of emergency alert information to non-English speaking Americans.</p> <p>On March 25, 2008, the Commission granted AT&T's request for a limited waiver of the December 3, 2007 deadline for wireline video providers to participate in EAS.</p> <p>On May 19, 2008, the Commission hosted a Summit on EAS. The panelists focused on the current state of the nation's EAS and what is needed to transition to a more robust Next Generation EAS to ensure that citizens receive accurate and timely information in emergencies.</p> <p>On June 6, 2008, the Commission released a guide to help small entities comply with the Next Generation EAS Regulations.</p>

EMERGENCY ALERTING			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Commercial Mobile Alert System (CMAS)</p> <p>PS Docket No.07-287</p> <p>DA 07-2935</p> <p>FCC 07-214</p> <p>FCC 08-99</p>	<p>Section 603 of the Warning, Alert and Response Network Act (WARN Act) required the FCC to develop technical standards and protocols to enable commercial mobile service providers to transmit emergency alerts to their subscribers.</p> <p>In April, 2008, the Commission adopted technical standards for the CMAS, including provisions regarding:</p> <ul style="list-style-type: none"> • Commercial Mobile Service (“CMS”) provider-controlled elements within the CMAS architecture; • Emergency alert formatting, classes, and elements; • Geographic targeting; • Accessibility for people with disabilities and the elderly; • Multi-language Alerting; • Availability of CMAS alerts while roaming; • Preemption of calls in progress; and • Initial implementation. 	<p>The CMAS is designed to allow important emergency messages to be widely circulated to wireless handsets.</p>	<p>On July 15, 2008, the Commission released an Order on Reconsideration and Erratum stating that CMS providers must begin development and testing of the CMAS in a manner consistent with the rules adopted in the First R&O no later than 10 months from the date that the Alert Aggregator / Alert Gateway makes the Government Interface Design specifications available.</p> <p>On August 7, 2008 in a Third Report and Order, the FCC (1) adopted notification requirements for CMS providers that elect not to participate, or to participate only in part, with respect to new and existing subscribers; (2) adopted procedures by which CMS providers may elect to transmit emergency alerts and to withdraw such elections; (3) adopted a rule governing the provision of alert opt-out capabilities for subscribers; (4) allowed participating CMS providers to recover costs associated with the development and maintenance of equipment supporting the transmission of emergency alerts; and (5) adopted a compliance timeline under which participating CMS providers must begin CMAS deployment.</p>

911 AND DISABILITY ACCESS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Wireless E911 Requirements</p> <p>PS Docket No. 08-51</p> <p>PS Docket No. 07-114</p> <p>CC Docket No. 94-102</p> <p>FCC 07-108</p> <p>FCC 07-166</p> <p>FCC 08-95</p>	<p>Enhanced 911 (E911) enables emergency service providers to accurately pinpoint the location of a 911 caller. The FCC currently requires CMRS providers to provide Public Safety Answering Points (PSAPs) with automatic number information and automatic location information.</p> <p>On June 1, 2007, the FCC adopted a NPRM regarding location accuracy and reliability requirements for wireless E911 services.</p> <p>On September 11, 2007, the FCC adopted an R&O on the geographic scope of the current wireless location accuracy requirements. Specifically, the FCC clarified that wireless carriers must meet E911 Phase II location requirements at a PSAP level by September 11, 2012. The FCC also adopted interim benchmarks under which carriers must fulfill its location accuracy requirements within each Economic Area by September 11, 2008 and within each Metropolitan Statistical Area and Rural Service Area level by September 11, 2010. Carriers also must demonstrate significant progress toward compliance at the PSAP-level, including achieving this requirement within at least 75 percent of the PSAPs the carrier serves, by September 11, 2010.</p>	<p>The wireless E911 rules were designed to improve the effectiveness and reliability of wireless 911 service by providing 911 dispatchers with additional information on wireless 911 calls.</p>	<p>The PSHSB held a Summit on the deployment and use of Next Generation 911 technology on February 6, 2008. The Summit included a list of recommendations for improving PSAP Call Center Operations.</p> <p>On April 11, 2008, the Commission issued a notice of inquiry asking for comment on the problem of non-emergency calls placed by non-service-initialized phones.</p> <p>On March 12, 2008, the Commission stayed the Economic Area-level compliance deadline until March 11, 2009.</p> <p>On March 25, 2008, the D. C. Circuit granted the requests of wireless carriers to stay the FCC's September 11 Order.</p> <p>On July 24, 2008 the FCC resolved seven issues raised by wireless manufacturer and telecommunications carrier defendants in their filings with the U.S. District Court for the Northern District of Illinois in an ongoing class action lawsuit regarding 911 call completion.</p>



911 AND DISABILITY ACCESS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>IP-Enabled Services E911 Requirements</p> <p>WC Docket No. 05-196</p> <p>CG Docket No. 03-123</p> <p>FCC 07-108</p> <p>FCC 08-78</p> <p>FCC 08-151</p>	<p>Providers of interconnected Voice over Internet Protocol (VoIP) service are required to supply enhanced 911 (E911) capabilities to their customers.</p> <p>In June 2007, the FCC released a Notice of Proposed Rulemaking, tentatively concluding that interconnected VoIP service providers should be required to employ an automatic location technology that meets the same accuracy standards that apply to CMRS carriers. The FCC also sought comment on the appropriate role of the Commission and states to regulate VoIP E911, and the need to expand obligations to non-interconnected VoIP services.</p>	<p>VoIP E911 rules may improve the effectiveness and reliability of VoIP 911 service by providing 911 dispatchers with additional information on VoIP 911 calls.</p>	<p>On March 19, 2008, the Commission released a Report and Order terminating all waivers of emergency call handling requirements for Internet-based telecommunications relay service (TRS) providers to ensure prompt access to emergency services.</p> <p>On June 11, 2008, the FCC adopted a system for assigning users of Internet-based TRS, ten-digit telephone numbers linked to the North American Numbering Plan to ensure, in part, that emergency calls placed by these users will be routed directly to the appropriate emergency services. The deadline for implementing the plan is December 31, 2008.</p>
<p>VoIP Disability Access Requirements</p> <p>WC Docket No. 04-36</p> <p>WT Docket No. 96-198</p> <p>CG Docket No. 03-123</p> <p>CC Docket No. 92-105</p> <p>FCC 07-110</p>	<p>Under Section 255 of the Communications Act, manufacturers of telecommunications equipment and providers of telecommunications service must ensure that their equipment or service is accessible to and usable by individuals with disabilities to the extent readily achievable.</p> <p>Section 225 requires, among other things, VoIP providers to contribute to the Telecommunications Relay Services Fund and to offer 711 abbreviated dialing for access to relay services.</p>	<p>The Section 255 requirements will ensure that individuals with disabilities will be able to take advantage of VoIP 911 services.</p>	<p>On June 15, 2007, the FCC adopted a Report and Order extending the disability access requirements of Sections 225 and 255 of the Communications Act to interconnected VoIP services and to manufacturers of specially designed equipment used to provide those services.</p>

CALEA			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
CALEA Wiretapping FCC 05-153 FCC 06-56 ET Docket No. 04-295 Report No. 2816 DA 07-2522 RM-11376	<p>Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. This law requires telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. CALEA applies to all telecommunications carriers as defined by Section 102(8) of CALEA, including entities engaged in the transmission or switching of wire or electronic communications as common carrier for hire. A telecommunications carrier must ensure that its equipment, facilities, and services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of meeting the assistance capability requirements.</p>	<p>CALEA preserves the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology.</p>	<p>Facilities-based broadband Internet access services and interconnected VoIP services must have complied with CALEA requirements by May 14, 2007.</p> <p>On May 15, 2007, the DOJ, FBI, and DEA filed a “Petition for Expedited Rulemaking” requesting the FCC to initiate a proceeding to find that the J-STD-025-B is deficient pursuant to Section 107(b) of CALEA and mandate the inclusion of four additional intercept capabilities in the J-STD-025-B with respect to CDMA2000 packet data wireless services. These capabilities are: packet activity reporting; provision of more granular mobile handset location information at the beginning and end of a communication; interception quality improvements, including security, performance and reliability requirements; and timing information (time stamping).</p> <p>The comment cycle on the J-STD-025-B safe harbor standard for CDMA wireless packet services is complete.</p>

KATRINA			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks</p> <p>FCC 07-107</p> <p>EB Docket No. 06-119</p> <p>WC Docket No. 06-63</p> <p>FCC 07-107</p> <p>EB Docket No. 06-119</p> <p>WC Docket No. 06-63</p>	<p>The Katrina Panel was established to review the impact of Hurricane Katrina on communications infrastructure and to recommend ways to improve network reliability and communication among emergency response services.</p> <p>On June 8, 2007, the FCC released an order (revised on reconsideration on October 4, 2007) in response to the Panel's recommendations. The FCC:</p> <ul style="list-style-type: none"> Required communications providers to (a) have emergency/back-up power for all assets regardless of the type of commercial power, unless precluded by law, public safety, or prior contract and (b) conduct analyses and submit reports on their back-up power compliance and the redundancy and resiliency of their 911 and E911 networks; Instructed the PSHSB, among other things, to develop and implement an awareness program to educate public safety agencies about alternative communications technologies, work with other federal agencies on developing credentialing standards for communications service providers and facilitating first responder interoperability, take steps to revitalize and publicize the current Emergency Alert system, and reach out to the emergency medical community to facilitate the resiliency and effectiveness of their emergency communications systems; and Extended regulatory relief from Section 272 of the Communications Act of 1934. 	<p>The Katrina Panel's recommendations and the directives in the ensuing order are designed to improve communication among emergency response services.</p>	<p>The PSHSB was required to report on its efforts 3 months and 9 months after the release of the June 8, 2007 order.</p> <p>Consistent with the FCC's June Order, the PSHSB launched a newly designed and automated Disaster Information Reporting System (DIRS) on September 11, 2007. DIRS is a voluntary, web-based system that communications companies, including wireless, wireline, broadcast, and cable providers, can use to report communications infrastructure status and situational awareness information during times of crisis.</p> <p>On July 8, 2008, U.S. Court of Appeals for the D.C. Circuit found that an appeal of the back-up power requirement was not ripe because the Office of Management and Budget (OMB) had not yet approved the information collection requirements contained in the rule's extensive reporting requirement. If the OMB approves the information collection requirements and a Court does not subsequently overturn the FCC's back-up power requirement, it will become effective after the information collection requirements are published in the Federal Register. Reports on compliance will be due within six months of the effective date. LECs and CMRS providers with less than the required backup power capacity will be required to comply with the rules or file a certified emergency backup power compliance plan within 12 months of the effective date.</p> <p>Comments on the resiliency and redundancy of 911 and E911 information collection requirements were due April 28, 2008.</p>



AIRPLANE COMMUNICATIONS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Aeronautical Mobile Satellite Service FCC 06-148 WT Docket No. 01-289	<p>Aeronautical Mobile Satellite Service (AMSS) is a mobile service between aeronautical stations and aircraft stations, or between aircraft stations. The service provides two-way communications, including broadband, onboard aircraft.</p> <p>The services, including certain frequency bands and technical standards used for this service, are coordinated internationally through the International Civil Aviation Organization to ensure the worldwide interoperability.</p> <p>In October 2006, the Commission adopted a Second R&O and FNPRM addressing and seeking comment on a number of issues pertaining to the Aviation Radio Service.</p>	<p>Many of the communications within this service are used for air traffic services and aeronautical operational control safety communications.</p> <p>Broadband capability for crews is intended to enhance aircraft operations through real time equipment and supply information, weather updates, and security monitoring.</p>	The comment cycle is complete.

MISCELLANEOUS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Rural Health Care Pilot Program FCC 07-198 DA 07-5018 WC Docket No. 02-60	In 2006, the FCC established a Rural Health Care Pilot Program (RHCPP) pursuant to § 254(h)(2)(A) of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, to create broadband telehealth networks to expand access to health care to rural and underserved American communities.	Improved telemedicine programs will help reduce costs and travel time for consumers, decrease medical errors, and enable health care providers to quickly share patient information.	<p>On November 1, 2007, the PSHSB, in conjunction with the U.S. Department of Health and Human Services, hosted a Health Care Summit on Emergency Communications, Response and Recovery. The Summit included an examination of the benefits of utilizing broadband networks and telemedicine.</p> <p>On November 19, 2007, the Commission released an Order selecting 69 participants for the Pilot Program. The participants will be eligible for funding to support up to 85% of the costs associated with the construction and servicing of state or regional broadband health care networks.</p>

BUREAUS/COMMITTEES			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Public Safety and Homeland Security Bureau</p> <p>FCC 06-35</p>	<p>On September 25, 2006, the FCC established the PSHSB. It is designed to address public safety functions that were previously dispersed among different bureaus. Those functions include public safety, homeland security, national security, disaster management, and emergency management and preparedness.</p>	<p>The PSHSB is the main bureau for FCC issues that deal with homeland security and public safety communications.</p>	<p>On September 25, 2007, PSHSB hosted a Summit on Communications Network Surge Management in Emergencies. The Summit examined how communications networks are managed during mass emergency situations.</p> <p>On November 1, 2007, PSHSB, in conjunction with the U.S. Department of Health and Human Services hosted a Health Care Summit on Emergency Communications, Response and Recovery. The Summit focused on hospital emergency communications plans and preparedness efforts and will examine the benefits of utilizing broadband networks and other communications infrastructure.</p> <p>On February 6, 2008, PSHSB hosted a Summit on 911 Call Center Operations and Next Generation Technologies. The Summit examined disaster preparation and response for 911 call centers and Public Safety Answer Points and the integration of new services and technologies.</p>



BUREAUS/COMMITTEES			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Intergovernmental Advisory Committee DA 07-2427 DA 07-4591	<p>The Intergovernmental Advisory Committee (IAC) is comprised of 15 representatives from local, state and tribal governments and “advises the Commission on a range of telecommunications issues for which their governments explicitly or inherently share responsibility or administration with the Commission.”</p> <p>The Commission reauthorized the IAC in February 2006 and rechartered the IAC in June 2007. The Commission’s authorization lasts for two years. There is an option for reauthorization every two years.</p>	The IAC addresses homeland security and public safety issues.	<p>On October 12, 2007, the Commission named members to the IAC.</p> <p>The IAC’s first meeting took place on December 12, 2007. Haley Barbour served as Chairman and Carlito Caliboso served as Vice-Chairman.</p>

BUREAUS/COMMITTEES			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
<p>Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities</p> <p>DA-07-4325</p> <p>DA-07-4622</p> <p>DA-07-4919</p> <p>DA-08-117</p>	<p>On September 7, 2007, the FCC and NTIA announced the establishment of a Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities.</p> <p>On February 4, 2008, the Joint Committee submitted its approved report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce. The Joint Committee recommended the following:</p> <ul style="list-style-type: none"> • The deployment of interoperable, standards-based broadband networks; • The establishment of a federal interagency coordinating committee; • A commitment by the federal government to develop uniform standards and protocols; • The development of common criteria for contracts and grants; • The improved use of telemedicine technology; • The improved coordination between existing systems; • The creation of a Command and Coordination System to track emergency vehicles; and • Fostering a regulatory environment. 	<p>The Committee addressed the communications needs of emergency medical and public health care facilities.</p>	<p>The Committee's Report was submitted to Congress in February 2008 and its work is complete.</p>

U.S. Congress

SPECTRUM			
Bill	Description	Relevance to Communications	Status/Notes
Crime Control and Prevention Act of 2007, S. 2237	<p>Authorizes appropriations for a number of federal, state, and local law enforcement and crime prevention programs. Includes provisions dealing with drug prevention, gun control, and computer fraud.</p> <p>Requires the Federal Communications Commission (FCC) to complete assignment of the 764-776 MHz and 794-806 MHz spectrum for public safety and law enforcement use.</p> <p>(See S. 2237 also in Interoperability and Cybersecurity & Critical Infrastructure sections.)</p>	Accelerates allocation of public safety spectrum.	<p>Sen. Joe Biden (D-DE) introduced S. 2237 on October 25, 2007, and it was referred to the Committee on the Judiciary.</p> <p>The FCC is continuing to implement 700 MHz and 800 MHz frequencies allocations to public safety agencies.</p>
Wireless Internet Nationwide for Families Act of 2008, H.R. 5846	Requires the FCC to license spectrum in two bands of frequencies of 20 MHz each. Eligible licensees must use the spectrum to provide broadband service free of charge to consumers and public safety agencies.	Seeks to expand access of broadband to more consumers, including public safety agencies.	Rep. Anna Eshoo (D-CA) introduced H.R. 5846 on April 17, 2008, and it was referred to the House Committee on Energy and Commerce.
Public Safety Broadband Authorization Act of 2008, H.R. 6055	Requires the FCC to modify the agreement for public safety broadband spectrum to require collaboration with the private sector and be managed by a non-profit that has no commercial interests in management and is representative of the public safety community.	Would impose requirements on the Public Safety Broadband Licensee (PSBL) and require the PSBL to work with the private sector	Rep. Jane Harman (D-CA) introduced H.R. 6055 on May 14, 2008, and it was referred to the House Committee on Energy and Commerce.

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
Fiscal Year 2009 Budget Resolution, S.Con.Res. 70	Sets forth the congressional budget for the federal government for Fiscal Year 2009. Does not appropriate actual funds; instead sets congressional spending goals in response to the President's budget request.	Includes a provision stating that increased homeland security funding will go, in part, to "equip, train and support first responders (including enhancing interoperable communications and emergency management)."	The Senate passed the resolution June 4, 2008. The House passed it June 5, 2008.
The Federal Emergency Management Advancement Act of 2007, S. 2214 The Federal Emergency Management Act of 2008, H.R. 6147	Establishes FEMA as an independent agency, separate from the Department of Homeland Security. Requires the FEMA Director to ensure acquisition of operable and interoperable communications by federal, state, and local governments and first responders. Requires FEMA Regional Administrators to assist in the development of operable and interoperable emergency communications capabilities.	Makes federal, state, and local emergency communications—both operability during an emergency and interoperability among systems—a priority.	Sen. James Inhofe (R-OK) introduced S. 2214 on October 22, 2007, and it was referred to the Committee on Homeland Security and Governmental Affairs. Rep. Tom Cole (R-OK) introduced H.R. 6147 on May 22, 2008, and it was referred to the House Committee on Transportation and Infrastructure and the House Committee on Homeland Security.
Crime Control and Prevention Act of 2007, S. 2237	Authorizes appropriations for a number of federal, state, and local law enforcement and crime prevention programs. Includes provisions dealing with drug prevention, gun control, and computer fraud. (See S. 2237 also in Spectrum and Cybersecurity & Critical Infrastructure sections.)	Authorizes \$1,000,000,000 in grants to state and local governments for interoperable communications equipment and planning.	Sen. Joe Biden (D-DE) introduced S. 2237 on October 25, 2007, and it was referred to the Committee on the Judiciary.

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
Public Safety Interoperability Implementation Act, H.R. 3116	Establishes the Public Safety Communications Trust Fund to make grants for interoperability and modernization of communications for public safety, fire, emergency, law enforcement, and crisis management within state and local government and non-profit entities. Will be funded from DTV Transition funds and proceeds of auctions of government-owned spectrum.	Provides grants to state and local first responders for communications interoperability.	Rep. Bart Stupak (D-MI) introduced H.R. 3116 on July 19, 2007, and it was referred to the House Committee on Energy and Commerce.
9/11 Can You Hear Me Now Act, H.R. 3119	Directs the Secretary of Homeland Security to procure a mobile communications system for the New York City Fire Department that is interoperable with other public safety communications systems and can work in all conditions and all locations in the city.	Provides new communications gear to the New York City Fire Department.	Rep. Carolyn Maloney (D-NY) introduced H.R. 3119 on July 26, 2007, and it was referred to the House Committee on Energy and Commerce.
National Urban Search and Rescue Response System Act of 2007, H.R. 4183	Creates a National Urban Search and Rescue Response System within the Department of Homeland Security to coordinate resources in the event of structural collapses in urban areas.	Provides grants to participating agencies for interoperable communications, among other things.	Rep. Loretta Sanchez (D-CA) introduced H.R. 4183 on November 14, 2007, and it was referred to the House Committee on Transportation and the Infrastructure and the House Committee on Homeland Security. The Homeland Security Subcommittee on Emergency Communications, Preparedness, and Response voted the bill out of the Subcommittee by voice vote on April 30, 2008.
Rural America Communications Expansion for the Future Act of 2008, H.R. 5862	Extends funds for public safety interoperability, 911 service, and telemedicine initiatives. Provides tax benefits and other incentives for broadband access in rural communities.	Authorizes funds for rural communities to obtain interoperable communications equipment and 911 service.	Rep. Tom Allen (D-ME) introduced H.R. 5862 on April 2, 2008, and it was referred to the House Ways and Means Committee, the House Committee on Agriculture, and the House Committee on Energy and Commerce.

HOMELAND SECURITY COMMUNICATIONS GRANTS

Bill	Description	Relevance to Communications	Status/Notes
Fiscal Year 2009 Homeland Security Appropriations Act, S. 3181	Appropriates funds to the Department of Homeland Security and other federal agencies. Also makes a number of grants for homeland security purposes.	Appropriates \$50,000,000 for the Interoperable Emergency Communications Grant Program.	Sen. Robert Byrd (D-WV) introduced S. 3181 on June 18, 2008, and it was referred to the Senate Committee on Appropriations. The Appropriations Committee approved it without amendment.
Fiscal Year 2009 Commerce, Justice, Science and Related Agencies Appropriations Act, S. 3182	Appropriates funds to the Department of Commerce, Department of Justice, and other agencies. Also appropriates money for many sources of grants for state and local law enforcement initiatives. Appropriates \$110,000,000 for law enforcement technology and interoperable communications. Appropriates \$121,651,000 for development of a national Integrated Wireless Network for federal law enforcement and for operation of the Land Mobile Radio legacy systems.	Appropriates funds for several law enforcement grant programs for the purchase of communications equipment.	Sen. Barbara Mikulski (D-MD) introduced S. 3182 on June 18, 2008, and it was referred to the Senate Committee on Appropriations. The Appropriations Committee approved it without amendment.
Tribal Government Homeland Security Coordination and Integration Act, H.R. 5530	Establishes an Office of Tribal Government Homeland Security and established a number of grants for homeland security initiatives in coordination with Indian tribes.	Requires the Secretary of Homeland Security to provide assistance to Indian tribes for acquisition of information technology for homeland security purposes and authorizes grants for addressing communications gaps.	Rep. Frank Pallone (D-NJ) introduced H.R. 5530 on March 4, 2008, and it was referred to the House Committee on Natural Resources and the House Committee on Homeland Security.
The Schools Empowered to Respond Act, H.R. 5766	Sets up within the Department of Homeland Security an Office of National School Preparedness and Response and provides a number of federal goals and support for school safety and emergency response.	Provides grants for communications equipment within schools for security plans.	Rep. Bob Etheridge (D-NC) introduced H.R. 5766 on April 28, 2008, and it was referred to the House Committee on Homeland Security and the House Committee on Transportation and Infrastructure.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

Bill	Description	Relevance to Communications	Status/Notes
Crime Control and Prevention Act of 2007, S. 2237	<p>Authorizes appropriations for a number of federal, state, and local law enforcement and crime prevention programs. Includes provisions dealing with drug prevention, gun control, and computer fraud.</p> <p>Authorizes \$80,000,000 for the Office of Domestic Preparedness for Critical Infrastructure Risk Assessment Planning and \$500,000,000 annually for grants to state and local governments for critical infrastructure protection.</p> <p>Authorizes \$30,000,000 for cyber crime prevention and enforcement.</p> <p>Establishes “Conspiracy to Commit Cyber Crimes” as a federal crime and fills perceived gaps in the federal cyber extortion law.</p> <p>(See S. 2237 also in Spectrum and Interoperability sections.)</p>	<p>Provides grants for protection of critical infrastructure.</p> <p>Reforms the laws designed to prevent cyber crimes and authorizes federal spending to help enforce those laws.</p>	Sen. Joe Biden (D-DE) introduced S. 2237 on October 25, 2007, and it was referred to the Committee on the Judiciary.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

Bill	Description	Relevance to Communications	Status/Notes
National Defense Authorization Act for Fiscal Year 2009, H.R. 5658	Authorizes funds for the Department of Defense and for the branches of the military for Fiscal Year 2009.	<p>Requires the Assistant Secretary of Defense for Networks and Information Integration to submit a report to Congress on the vulnerability of Future Combat Systems' communications to enemy attack, national disaster, or other contingencies.</p> <p>Requires the Secretary of Defense to assess the military's need for commercial satellite capabilities and to create an acquisition strategy.</p>	Rep. Ike Skelton (D-MO) introduced H.R. 5658 on March 31, 2008. The House passed H.R.5658 on May 22, 2008, by a vote of 384-23. The legislation is currently on the Senate Legislative Calendar.

EMERGENCY ALERTING			
Bill	Description	Relevance to Communications	Status/Notes
Integrated Public Alert and Warning System Modernization Act of 2008, H.R. 6038	Requires the Director of FEMA to create a new, modern emergency alert system to ensure people can receive all relevant alerts and warnings. The system must incorporate multiple communications technologies, aim to provide alerts to as many people as possible, and promote local/regional partnerships.	Modernizes the emergency alert communications system.	Rep. Sam Graves (R-MO) introduced H.R. 6038 on May 13, 2008, and it was referred to the House Committee on Transportation and the Infrastructure.
Alerting Lives through Effective and Reliable Technological Systems Act of 2008 (ALERTS Act), H.R. 6392	Requires the Secretary of Homeland Security to establish a national integrated public alert and warning system that reaches as many people as possible and is resilient in the event of natural or manmade disaster. The system would include a program to alert the public through commercial mobile devices and the legislation would establish a pilot program for this system.	Modernizes the emergency alert communications system and seeks to incorporate a number of new technologies into the public alert system.	Rep. Henry Cuellar (D-TX) introduced H.R. 6392 on June 26, 2008, and it was referred to the House Committee on Transportation and the Infrastructure and the House Committee on Homeland Security.

COMMUNICATIONS SURVEILLANCE			
Bill	Description	Relevance to Communications	Status/Notes
National Security Letter Reform Act of 2007, S. 2088	<p>Places restrictions on the use of National Security Letters issued by the FBI to electronic communications service providers, financial institutions, and consumer credit reporting agencies for the production of specified records and information about customers or subscribers.</p> <p>Allows the issuance of a National Security Letter only where: (1) the records sought relate to an ongoing, authorized and specifically identified national security investigation (other than a threat assessment); and (2) there are specific and articulable facts for believing that such records pertain to a suspected agent of a foreign power and such agent's activities.</p>		<p>Sen. Russ Feingold (D-WI) introduced S. 2088 on September 25, 2007, and it was referred to the Committee on the Judiciary.</p> <p>The Committee held a hearing, but it has taken no other action.</p>
FISA Improvement Act of 2007, S. 2440	<p>Reauthorizes and makes a number of changes to FISA. Allows the Attorney General (AG) and the Director of National Intelligence (DNI) to authorize surveillance of persons outside the U.S.</p> <p>Revises the court review process of applications for domestic surveillance.</p> <p>Contained the legislation passed by the Senate Judiciary Committee except for the immunity provision.</p>	Does not provide immunity to communications companies.	Sen. Harry Reid (D-NV) introduced S. 2440 on December 10, 2007, and it was placed on the Senate calendar.
Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007, S. 2441	<p>Reauthorizes and makes a number of changes to FISA. Allows the AG and the DNI to authorize surveillance of persons outside the U.S.</p> <p>Revises the court review process of applications for domestic surveillance.</p> <p>Contained the legislation passed by the Senate Intelligence Committee.</p>		Sen. Harry Reid (D-NV) introduced S. 2441 on December 10, 2007, and it was placed on the Senate calendar.

COMMUNICATIONS SURVEILLANCE			
Bill	Description	Relevance to Communications	Status/Notes
Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, S. 2248	<p>Reauthorizes and makes a number of changes to FISA.</p> <p>Authorizes the AG and the DNI to acquire foreign intelligence information from non-U.S. citizens outside the U.S. for a period up to one year.</p> <p>Allows the AG to authorize the emergency employment of electronic surveillance for up to 168 hours without a judicial order.</p> <p>Requires the FISA Court to review and certify targeting and minimization procedures for acquiring intelligence information.</p>	Granted immunity to communications companies for providing information to the U.S. government.	<p>Sen. Jay Rockefeller (D-WV) introduced S. 2248 on October 26, 2008, and it was referred to the Committee on the Judiciary. The Judiciary Committee reported it with a substitute.</p> <p>The Senate passed it with amendment by a vote of 68-29, but they incorporated it into H.R. 3773 as an amendment.</p>
Foreign Intelligence Surveillance Act Amendments, H.R. 3138	<p>Redefines “electronic surveillance” as 1) the installation or use of surveillance device and a particular person believed to be in the United States 2) or the intentional acquisition of a communication when the person has a reasonable expectation of privacy and a warrant would be required.</p> <p>Would effectively exempt some NSA activity from the requirements of FISA with the definition of surveillance narrowed.</p>		Rep. Heather Wilson (R-NM) introduced H.R. 3138 on July 24, 2007, and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence.
Foreign Intelligence Surveillance Act Update, H.R. 3321	<p>Amends FISA to redefine “electronic surveillance” such that it does not include surveillance directed at someone outside the United States.</p> <p>Authorizes the AG and the DNI, for periods up to one year, to acquire foreign intelligence information concerning persons outside the United States under specified procedures subject to review by the FISA Court.</p>		Rep. Pete Hoekstra (R-MI) introduced H.R. 3321 on August 2, 2007, and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence.

COMMUNICATIONS SURVEILLANCE			
Bill	Description	Relevance to Communications	Status/Notes
<p>Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, H.R. 3356</p> <p>Protect America Act of 2007, S. 2011</p> <p>(Identical Bills)</p>	<p>Amends FISA to provide that a court order is not required for acquiring communications between non-U.S. persons not in the U.S.</p> <p>The Attorney General, upon authorization of the President, can apply to the FISA Court for a surveillance authorization lasting up to one year for the acquisition of communications of persons outside the United States who are non-U.S. persons. The AG can authorize such surveillance without a court order for up to 15 days if the AG determines that an emergency situation exists.</p>		<p>Rep. Silvestre Reyes (D-TX) introduced H.R. 3356 on August 3, 2008, and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence.</p> <p>It was brought to the floor under Suspension of the Rules (where it required 2/3 vote to pass) and failed by a vote of 218-207.</p> <p>Sen. Carl Levin (D-MI) introduced S. 2011 on August 3, 2007. The Senate defeated it by a vote of 43-45.</p>
<p>Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 3773</p>	<p>Reauthorizes FISA with a number of changes. Clarifies that no court warrant is required to intercept communications of non-U.S.</p> <p>persons when both ends of the communication are outside the United States. Creates a program of court authorized targeting of non-U.S. persons outside the United States.</p> <p>The House version of H.R. 3773 did not provide immunity to communications companies for sharing information with the government.</p>		<p>Rep. John Conyers (D-MI) introduced H.R. 3773 on October 9, 2007, and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence.</p> <p>Both committees reported the bill, and the House passed it by a vote of 227-189 on November 15, 2007. The Senate passed it with an amendment (replacing the language of with bill with S. 2248) by unanimous consent on February 12, 2008. The House then amended the version passed by the Senate, and the amended version passed the House 213-197. The Senate did not take it up for consideration of the House amendment.</p>

COMMUNICATIONS SURVEILLANCE			
Bill	Description	Relevance to Communications	Status/Notes
Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304	<p>Represented the compromise version of the FISA Reauthorization legislation.</p> <p>Increases the role of the FISA Court in reviewing and approving targeting and minimization procedures, ensures that traditional FISA warrant rules still apply for purely domestic communications, and requires FISA Court orders prior to surveillance or physical searches of U.S. persons abroad.</p> <p>Provides Court review of procedures before surveillance begins unless there are exigent circumstances, in which case the AG must seek approval from the FISA Court within seven days.</p> <p>This bill will sunset the legislation in four and a half years.</p>	Grants telecommunications companies immunity from civil liability, provided a federal district court determines that the AG's certification of immunity applies and is supported by substantial evidence.	<p>Rep. Silvestre Reyes (D-TX) introduced H.R. 3356 on June 19, 2008, and it was referred to the House Committee on the Judiciary and the House Permanent Select Committee on Intelligence.</p> <p>It passed the House by a vote of 293-129. The Senate passed the bill unamended by a vote of 69-28. President Bush signed the bill into law on July 10, 2008.</p>

E-911 AND CITIZEN EMERGENCY COMMUNICATIONS

Bill	Description	Relevance to Communications	Status/Notes
Food and Energy Security Act of 2007 ("The Farm Bill"), S. 2302	Reauthorizes a number of agricultural support, conservation, and nutrition programs. In addition, provides grants and loans to states and rural communities to provide for energy, educational, and technology access/development in rural communities.	Authorizes loans to state governments, localities, and emergency equipment providers for expansion or improvement of 911 access and interoperable emergency communications in rural areas.	Sen. Tom Harkin (D-IA) introduced S. 2302 on November 2, 2007. S. 2302 was incorporated into H.R. 6124 (see below).
Secure America through Verification and Enforcement Act of 2007 (SAVE Act), S. 2366 & S. 2368 (identical bills)	Establishes a number of border security measures.	Requires the Secretary of Homeland Security to create and carry out a plan to use satellite and other communications means in order for clear and secure communications among federal, state, and local border protections officials. Requires the Secretary to use radio technology that will allow for encrypted communications between border protection officials.	Sen. David Vitter (R-LA) introduced S. 2366 on November 15, 2007, and it was referred to the Committee on Finance. Sen. Mark Pryor (D-AR) introduced S. 2368 on November 15, 2007, and it was referred to the Committee on Finance.
Subway Cell Access Act, H.R. 2972	Directs the FCC to require that all wireless phone service providers ensure the ability to use 911 service at underground subway stations in any service area where the provider services the ground level.	Requires 911 accessibility for wireless phones in underground subway stations.	Rep. Anthony Weiner (D-NY) introduced H.R. 2972 on July 10, 2007, and it was referred to the House Committee on Energy and Commerce.

E-911 AND CITIZEN EMERGENCY COMMUNICATIONS

Bill	Description	Relevance to Communications	Status/Notes
911 Modernization and Public Safety Act of 2007, H.R. 3403	Requires IP-enabled voice service providers (VOIP) to provide 911 service and E-911 service to their subscribers.	Expands E-911 to VOIP service providers.	Rep. Bart Gordon (D-TN) introduced H.R. 3403 on August 13, 2007, and it was referred to the House Committee on Energy and Commerce. The House passed it 406-1 on November 13, 2007, and the Senate passed it with amendment by unanimous consent on June 16, 2008. The House agreed with the Senate amendment on June 23, 2008, and President Bush signed it into law on July 23, 2008 (Public Law 110-283).
Rural America Communications Expansion for the Future Act of 2008, H.R. 5682	Provides tax benefits and other incentives for broadband access in rural communities.	Provides funds for rural 911 access.	Rep. Tom Allen (D-ME) introduced H.R. 5862 on April 2, 2008, and it was referred to the House Ways and Means Committee, the House Agriculture Committee, and the House Energy and Commerce Subcommittee on Telecommunications and the Internet.
National Silver Alert Act, H.R. 6064	Encourages states to adopt a Silver Alert plan that would aid in the recovery of missing senior citizens through coordination of state and local public safety and health agencies. Creates a grant program and minimum standards that would help states in setting up these programs.	States can use grant funds for new communications technology in setting up their Silver Alert program.	Rep. Lloyd Doggett (D-TX) introduced H.R. 6064 on May 15, 2008, and it was referred to the House Committee on the Judiciary. Nine states currently have Silver Alert programs in place.

E-911 AND CITIZEN EMERGENCY COMMUNICATIONS

Bill	Description	Relevance to Communications	Status/Notes
Food, Conservation, and Energy Act of 2008, H.R. 6124	<p>Reauthorizes a number of agricultural support, conservation, and nutrition programs.</p> <p>In addition, provides grants and loans to states and rural communities to provide for energy, educational, and technology access/development in rural communities.</p>	<p>Authorizes loans to state governments, localities, and emergency equipment providers for expansion or improvement of 911 access and interoperable emergency communications in rural areas.</p> <p>Provides loans and loan guarantees for broadband service providers to build out to rural communities.</p> <p>Requires the FCC to create a Rural Broadband Strategy.</p>	<p>Rep. Collin Peterson (D-MN) introduced H.R. 6124 on May 22, 2008, and it was referred to the House Committee on Agriculture and the House Committee on Foreign Affairs.</p> <p>The House passed H.R. 6124 by a vote of 306-110, and the Senate passed it by a vote of 77-15.</p> <p>President Bush vetoed the legislation on June 18, 2008.</p> <p>The House and Senate both voted to override the veto, by votes of 317-109 and 80-14, respectively. It became Public Law 110-246.</p>

BORDER & PORT SECURITY			
Bill	Description	Relevance to Communications	Status/Notes
Secure America Through Verification and Enforcement Act of 2007 (SAVE Act), S. 2366 & S. 2368 (identical bills)	Establishes a number of border security measures.	<p>Requires the Secretary of Homeland Security to create and carry out a plan to use satellite and other communications means in order for clear and secure communications among federal, state, and local border protections officials.</p> <p>Requires the Secretary to use radio technology that will allow for encrypted communications between border protection officials.</p>	<p>Sen. David Vitter (R-LA) introduced S. 2366 on November 15, 2007, and it was referred to the Committee on Finance.</p> <p>Sen. Mark Pryor (D-AR) introduced S. 2368 on November 15, 2007, and it was referred to the Committee on Finance.</p>
Emergency Port of Entry Personnel and Infrastructure Funding Act of 2007, S. 2474	Hires additional border protection personnel and constructs additional ports of entry along the northern and southern U.S. borders.	Requires the Secretary of Homeland Security to purchase two-way communication and satellite-enabled devices to enable communications among ports of entry, patrol, and inspection stations, other Federal, State, local and tribal law enforcement agencies.	Sen. John Cornyn (R-TX) introduced S. 2474 on December 13, 2007, and it was referred to the Senate Committee on Homeland Security and Government Affairs.

U.S. Department of Homeland Security

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
National Communications System (Generally)	<p>The NCS assists the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack & recovery and reconstitution.</p> <p>The NCS has created a number of different services. NS/EP Priority Telecommunications (GETS, TSP, WPS); National Coordinating Center for Telecommunications (ACN, SHARES); Telecom ISAC; Emergency Response Training (Planning, Training, and Exercise Support); Individual Mobilization Augmentee.</p>	Provides for emergency federal oversight for federal and non-federal communications.	<p>After nearly 40 years with the Secretary of Defense serving as its Executive Agent, the National Communications System was transferred to the Department of Homeland Security (DHS).</p> <p>In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure.</p> <p>On April 28, 2008, James J. Madon became the Director of NCS.</p>

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
National Security Telecommunications Advisory Committee (NSTAC)	<p>For 25 years, the NSTAC has provided the U.S. Government with industry advice in the areas of national security and emergency preparedness (NS/EP).</p> <p>The NSTAC brings together industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies to provide the President with expertise and advice.</p>	The NSTAC goal is to ensure reliable telecommunication links in the course of emergencies.	<p>On January 16, 2007, the NSTAC issued a Report to the President outlining five recommendations on how to improve emergency communications and interoperability.</p> <p>On August 16, 2007, the NSTAC issued a Report to the President recommending that DHS coordinate with Allied governments to develop a global framework of response strategies.</p> <p>In response to a White House request, on February 28, 2008, the NSTAC issued a Report to the President on the commercial communications infrastructure's reliance on the Global Positioning System (GPS).</p> <p>The NSTAC last met with the President and the Chamber of Commerce on May 1, 2008.</p>

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
National Emergency Communications Strategy	In February 2006, DHS submitted to the President a document entitled the <i>Federal Response to Hurricane Katrina: Lessons Learned</i> , which outlined numerous lessons learned and identified 17 challenges facing the Federal Government, including communications and critical infrastructure protection. In response, the President directed NCS to organize an interagency group to begin development of a national emergency communications strategy. The NCS worked in partnership with a Federal interagency working group to develop a strategy and submitted the interagency interim <i>National Emergency Communications Strategy</i> to the President for further review and consideration on May 17, 2006.	Provides a framework for future U.S. Government emergency response planning efforts and informs revisions to key policy documents governing emergency communications support.	Interim strategy submitted to the President for consideration and review. In January 2007, the President's National Security and Telecommunication Advisory Committee (NSTAC) submitted a report to the President on Emergency Communications and Interoperability. In this Report, the NSTAC recommended that several elements be incorporated into the National Emergency Communications Strategy, including yearly benchmarks for achieving defined interoperability objectives, the development of large-scale state and regional shared public safety networks and federal grants, and nationwide outreach, among other things.

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
National Infrastructure Protection Plan (NIPP) and, specifically, Communications SSP	<p>To address the pre-existing threat of natural disasters, while factoring in the new threat of terrorism, the Department of Homeland Security (DHS) released the National Infrastructure Protection Plan (NIPP) in June 2006. The plan provides a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. The NIPP coordinates Federal departments and agencies; State, local, and tribal governments; private sector owners and operators; and international partners.</p> <p>To implement the NIPP, Sector-Specific Agencies (SSAs) for each of the 17 critical infrastructure and key resources (CI/KR) sectors are partnering with State, local, and tribal governments, and industry to create and implement Sector-Specific Plans (SSPs).</p>	The Communications SSP describes a collaborative effort among the private sector, Federal Government, and State governments to protect the Nation's communications infrastructure. This collaboration will result in the assessment of risk to the communications architecture and its functions that will help prioritize protection initiatives and investments within the sector and aid the identification of critical assets against specific threats.	The Communications SSP was released in May 2007. It results from a close collaboration among the NCS, the Communications Sector Coordinating Council, and the Communications Government Coordinating Council (GCC). It provides a framework for industry and government partners to develop a coordinated protection strategy.
Route Diversity Project (RDP)	The Route Diversity Project was established to develop a route diversity methodology and route diversity analysis capability that could analyze Federal agencies' telecommunications resiliency and redundancy. The RDP also researches and demonstrates various technical approaches that could be used to provide this service.	Aids federal agencies in improving the resiliency and redundancy of their communications networks.	<p>The RDP continually investigates new solutions for creating a resilient network. Evaluations on Free Space Optics and satellite communications have been released. Evaluations of service offerings and white papers on various technologies are expected to be released. See http://www.ncs.gov/rdp/index.html under "Technology Research."</p> <p>Third parties may partner with the RDP to evaluate a technology or service.</p>

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Communications Resource Information Sharing (CRIS)	<p>The CRIS initiative establishes an information source that identifies transportable communications equipment, over-the-counter services, and fixed communications networks of the Federal government that could be used on a shared basis with other Federal organizations to support NSEP requirements.</p> <p>CRIS is open to all NCS member organizations (23 Federal departments and agencies) and their affiliates on a voluntary basis. Identification of telecommunications resources for use in CRIS is also on a voluntary basis, and the sharing of such resources is not to interfere with an organization's mission.</p>	Facilitates the shared use of communications assets, services, and capabilities during an emergency.	<p>The Executive Office of the President approved CRIS in February 1996.</p> <p>The NCS CRIS Working Group guides the CRIS initiative. The Chief, Operations Division (N3), NCS provides day-to-day administration of CRIS.</p> <p>Twenty-six Federal and industry organizations contribute resources to CRIS.</p>
Communications Infrastructure Information Sharing and Analysis Center (ISAC)	The ISAC's mission is to facilitate voluntary collaboration and information sharing among Government and industry in support of the protection of the nation's critical infrastructure by gathering information on vulnerabilities, threats, intrusions, and anomalies from multiple sources and performing analyses with the goal of averting or mitigating impact upon the telecommunications infrastructure.	Facilitates the sharing of information among Government and industry so that the impact of a national disaster on telecommunications infrastructure can either be averted or mitigated.	<p>Currently, there are 41 members.</p> <p>The Communications ISAC is available 24/7.</p>
Network Security Information Exchange (NSIE)	The NSIE is an industry-Government partnership that was established to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures.	Facilitates the sharing of information and ideas among Government and industry regarding network security.	The NSIE occasionally holds ad hoc sessions to discuss security technologies and their implementation. The NSIE also provides immediate assistance to NSIE member organizations when urgent security concerns arise.

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Modeling, Analysis and Technology Assessment	<p>NCS uses a number of modeling and analysis techniques and applications to conduct technical studies or analyses for the purpose of identifying improved approaches that may assist Federal entities in fulfilling NSEP objectives.</p> <p>For example, the Network Design and Analysis Capability (NDAC) analyzes different operational aspects of telecommunications networks, thereby enabling NCS to review the operation of the public switched network.</p> <p>NCS is also modeling and analyzing a variety of other technologies, including next generation networks, the Internet, supervisory control and data acquisition systems, and a next generation priority services experimental testbed environment. NCS has also developed a Technology Assessment Network, which enables the evaluation of cutting edge technology without jeopardizing existing development or production of systems and a Technology Assessment and Data Analysis Cell, which will provide NCS with a fully accredited facility capable of evaluating contract deliverables and products, hosting applications and databases, providing component-level simulation, participating in community research projects, and training.</p>	<p>These techniques detect and help mitigate damage caused by disasters and assists in reconstitution of telecommunications networks. They also assist in the development of future networks.</p>	<p>These activities remain ongoing and the techniques are continually refined and expanded through software updates and application development.</p>

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Advanced Technology Group (ATG)	The ATG investigates new and emerging technologies with the objective of making them available to Government during national emergencies or crises. Specifically, the ATG has performed studies on Telecommunications Electromagnetic Disruptive Effects and has published a number of technical reports concerning vulnerability issues associated with the telecommunications infrastructure and emerging wireless and wireline communications technologies, such as satellite communications, the Alerting and Communications Network, and the Global Positioning System, and their impact on NSEP telecommunications services.	Furtheres the use of new and evolving technologies by government agencies during emergencies.	The ATG's studies remain ongoing. Among other things, the ATG is introducing concepts to solve credentialing using satellite technologies, in addition to investigating priority satellite communications for NSEP.
Continuity Communications Working Group	The Continuity Communications Working Group addresses stove-piped systems and the lack of interoperability between Federal Executive Branch departments and agencies in their continuity communications infrastructure.	Facilitates the continuity of federal government communications.	In 2006, the Continuity Communications Working Group was reconstituted under the NCS' Committee of Principals. The Working Group's efforts remain ongoing.
National Coordinating Center for Telecommunications (NCC)	The NCC is the primary mechanism within the NCS for fulfilling the emergency response role. The NCC's mission is to assist in the initiation, coordination, restoration and reconstitution of NSEP telecommunications service or facilities under all conditions, crises, and emergencies.	Coordinates the restoration and provisioning of NSEP telecommunication services and facilities during natural disasters and armed conflicts.	The NCC's work is ongoing.

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Alerting and Coordination Network (ACN)	The ACN was designed to provide a survivable emergency communications network connecting critical telecommunications service providers' network operations and/or emergency operation centers with key federal entities.	Provides a stable voice communications network for restoration coordination, priority transmissions, and incident reporting when the public switched network is inoperable.	The NCS is in the process of implementing new ACN capabilities and technical architecture.
National Response Framework (NRF)	The National Response Framework (NRF) replaced the National Response Plan on March 28, 2008. The Framework, which focuses on response and short-term recovery, articulates the doctrine, principles and architecture by which our nation prepares for and responds to all-hazard disasters across all levels of government and all sectors of communities. The Framework is responsive to repeated federal, state and local requests for a streamlined document that is shorter, less bureaucratic and more user-friendly.	Addresses the role of communications networks and personnel during emergencies and the necessity for accurate and timely communications among government users and with the public.	Information on the NRF can be accessed from the NRF Resource Center at http://www.fema.gov/emergency/nrf/ .
National Strategy to Secure Cyberspace	The National Strategy to Secure Cyberspace outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity.	This strategy is part of an overall effort to protect the Nation by engaging and empowering Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.	The National Strategy to Secure Cyberspace was released in 2003.

NETWORK SECURITY AND RELIABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Cyber Security Awareness Month	The National Cyber Security Alliance, a consortium of government agencies and private industry sponsors, has declared October as National Cyber Security Awareness Month. National Cyber Security Awareness Month is a national campaign designed to increase the public's awareness of cyber security and crimes issues, so that users can take precautions to avoid these threats on the Internet.	Maintaining cyber security is essential to protect the integrity and functioning of the nation's communications infrastructure.	National Cyber Security Awareness Month began in October 2004.
Cyber Storm Exercises	DHS is conducting a series of congressionally mandated exercises that stimulate a coordinated cyber attack on information technology, communications, chemical and transportation systems.	The Cyber Storm exercises help to ensure that the public and private sectors are prepared for an emergency response to a cyber attack.	The first Cyber Storm was held in February of 2006. Cyber Storm II, the largest cyber security exercise to date, was held on March 10-14, 2008 and included five countries, nine states, 18 federal departments and agencies, and more than 40 private companies.

PRIORITY SERVICE			
Initiative	Description	Relevance to Communications	Status/Notes
Priority Services Working Group (PSWG)	The PSWG was established to undertake (1) an evaluation of the NCS' GETS, TSP, and WPS programs; (2) an examination of priority service outreach efforts; (3) an assessment of cost issues; and (4) an analysis of the potential impact of future technologies on priority services programs.	Provides recommendations on how priority service programs can be improved.	The PSWG's review is ongoing. In 2006, the PSWG completed a report on the Telecommunications Service Priority Program.
Telecommunications Service Priority (TSP)	<p>The TSP program provides the framework for the priority restoration and provisioning of any qualified national security and emergency preparedness (NSEP) telecommunications services.</p> <p>NSEP services are those services used to maintain a state of readiness or manage any emergency (local, national, or international) that harms the population, damages property, or threatens the NSEP posture of the U.S.</p> <p>A restoration priority is assigned to new or existing telecommunications services to ensure restoration before non-TSP services. Priority restoration should be assigned to a new service when interruptions may have a serious, adverse effect on the supported NSEP function.</p> <p>A provisioning priority facilitates priority installation of new telecommunications services. Provisioning on a priority basis becomes necessary when a service user has an urgent requirement for a new NSEP service that must be installed quickly.</p>	Facilitates emergency provisioning and repair of certain communications services.	<p>In 1988, the FCC issued a Report and Order (FCC 88-341) establishing the TSP Program. Currently there are over 109,000 total active TSP assignments in support of NSEP communications. During FY 2006, over 32,000 TSP codes were added, changed or revoked. Additionally, the TSP user base increased by approximately 128 new organizations, bringing the total number of organizations with active TSP codes to over 680.</p> <p>In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to explore enhancements to the TSP program to accommodate expanded requests from national NSEP users of wireless telecommunications services at critical sites.</p>

PRIORITY SERVICE			
Initiative	Description	Relevance to Communications	Status/Notes
Government Emergency Telecommunications Service (GETS)	<p>Provides NSEP users with emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) when their normal telecommunications means are unavailable or congested during an emergency.</p> <p>GETS calls receive priority treatment through enhanced routing, controls such as trunk queuing, trunk sub-grouping, and trunk reservation, and through exemption from restrictive network management controls used to reduce network congestion.</p> <p>GETS is accessed through a universal access number and Personal Identification Number (PIN) card. Once the caller is authenticated, his or her call receives priority treatment.</p>	Facilitates access to wireline communications services by certain entities in an emergency.	<p>The President directed the Office of the Manager, NCS (OMNCS) to develop GETS.</p> <p>On 9/11, 18,000 GETS calls were made (10,000 in NY and DC), and the call completion rate exceeded 95%. During the 2001 Nisqually Earthquake near Seattle, there were 400 successful GETS calls.</p> <p>As of September 30, 2006, there were 140,743 active GETS cards—an increase of 30,283 cards since September 2005.</p> <p>In February, 2008, NCS began a campaign to expand the use of GETS by increasing the number of GETS cards among emergency personnel.</p>

PRIORITY SERVICE			
Initiative	Description	Relevance to Communications	Status/Notes
Wireless Priority Service (WPS)	<p>During emergencies, cellular networks can experience congestion due to increased call volumes and/or damage to network facilities. Wireless Priority Service was developed to provide priority for emergency calls made from cellular telephones.</p> <p>Wireless Priority Service is implemented as software enhancements to cellular networks, and is being deployed by cellular service providers in their coverage areas throughout the United States.</p>	Facilitates access to wireless communications services by certain entities in an emergency.	<p>As of September 30, 2006, there were 38,668 authorized WPS users—a 51 percent increase since September of 2005.</p> <p>In January 2007, the President's National Security Telecommunications Advisory Committee recommended that the President direct DHS to expand and enhance use of the WPS program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi-carrier WPS end-to-end solutions that facilitate the rapid restoration of essential wireless network elements.</p> <p>In February, 2008, NCS began a campaign to expand the use of WPS by increasing the number of WPS subscriptions among emergency personnel.</p>

EMERGENCY ALERTING			
Initiative	Description	Relevance to Communications	Status/Notes
Digital Emergency Alert System (DEAS)	The Digital Emergency Alert System is testing how the digital capabilities of the nation's public radio and television stations and other networks—combined with the voluntary participation of cell phone service providers; public and commercial radio and television broadcasters; satellite radio, cable, and Internet providers; and equipment manufacturers—can be used to provide alert and warning information to the public and to disaster support personnel.	Utilizes existing communications infrastructure to expand the alerting system so that everyone, regardless of location or time of day, will receive emergency information.	<p>The national DEAS pilot will run for 1 year beginning in January 2007, with all public broadcasting stations (over 300 nationwide) to be DEAS-enabled by December 2007</p> <p>Overall, the new warning system is expected to cost \$4.5 million to test and deploy nationally, and \$1 million annually to maintain.</p>
Shared Resources High Frequency Radio Program (SHARES)	<p>SHARES brings together existing HF radio resources of federal, state, and industry organizations to provide a single, interagency emergency message handling system for Federal departments and agencies.</p> <p>Certain conditions must exist to use SHARES, including: the information must support NSEP requirements; the information must be communicated to a Federal entity and be of critical importance to the Federal government, the entity's mission, and/or involve the preservation of life and property; the primary means of communications must be inoperative or unavailable for use; and the processing of SHARES message traffic must not interfere with the primary mission requirements of the SHARES participants.</p> <p>To access SHARES, a user contacts the nearest SHARES station listed in the SHARES Directory and requests assistance in processing a SHARES message.</p> <p>SHARES is available on a 24/7 basis.</p>	More than 250 designated frequencies have been authorized for use in SHARES.	<p>SHARES stations are located in every state and at 20 overseas locations.</p> <p>194 emergency planning and response personnel participate.</p> <p>A SHARES Bulletin is published periodically to keep members updated on program activities.</p> <p>The SHARES HF Interagency Working Group, consisting of 154 members representing 110 organizations, conducts three nationwide readiness exercises each calendar year, which provides personnel training on operating procedures and various message formats, expands SHARES awareness within the Federal emergency response community and assesses the interoperability of new HF technologies.</p>

OTHER			
Initiative	Description	Relevance to Communications	Status/Notes
People Access Security Service (PASS) System. DHS Proposes to Expand the Use of Vicinity RFID in Implementing Western Hemisphere Travel Initiative	<p>The Department of Homeland Security (DHS), in conjunction with the Department of State's proposed rulemaking on the new PASSport card, announced in October 2006 that it proposes to expand the use of vicinity radio frequency identification (RFID) technology at U.S. ports of entry. The vicinity RFID technology, to be compatible with the PASSport card, would allow a travel document to be read from several feet away as a vehicle approaches inspection.</p> <p>The proposed PASSport card would serve as an alternative to a traditional passport book for use by U.S. citizens who cross the land borders and travel on cruises to Canada, Mexico and the Caribbean. It would provide evidence of identity and citizenship, be convenient to carry, and cost less than the traditional passport book.</p>	PASS utilizes communications technology to address border security issues.	The proposed regulations of the PASSport card were published by the Department of State in the Federal Register on October 17, 2006. The comment cycle on this Proposed Rule has closed.

OTHER			
Initiative	Description	Relevance to Communications	Status/Notes
National Emergency Communications Plan (NECP)	On July 31, 2008, DHS released a National Emergency Communications Plan (NECP), the nation's first strategic plan designed to improve emergency communications. The NECP outlines goals and recommendations to ensure a minimum level of interoperability for federal, state, and local agencies.	The NECP will improve emergency communications by promoting a coordinated, nationwide strategy.	NECP establishes the following goals: <ul style="list-style-type: none"> • By 2010, 90% of high-risk areas within the Urban Area Security Initiative (UASI) are able to demonstrate response-level emergency communications within one hour of a routine event. • By 2011, 75% of non-UASI jurisdictions are able to demonstrate response level emergency communications within one hour of a routine event. • By 2013, 75% of all jurisdictions are able to demonstrate response-level emergency communications within three hours of a significant event.

U.S. Department of Justice

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
Integrated Wireless Network (IWN)	<p>IWN is a joint effort by the DOJ, DHS, and the Treasury to provide a consolidated nationwide federal wireless communications service that replaces stand alone component systems and supports first responders and law enforcement with integrated communications services (voice, data, and multimedia).</p> <p>IWN is governed by the IWN Executive Board, which is comprised of the CIOs from DOJ, DHS, and Treasury.</p> <p>The government estimates that IWN should take between 5-10 years to complete. The estimated funding for IWN is \$2.5 billion (however, the ceiling is \$10 billion).</p> <p>The government estimates that IWN will serve over 80,000 law enforcement users and will operate through 2,500 sites.</p>	IWN will implement solutions to provide federal agency interoperability with appropriate links to state, local, and tribal public safety and homeland security entities.	<p>General Dynamics has been selected as the IWN integrator. The contract with General Dynamics is also available for use by the other IWN partners.</p> <p>On February 4, 2008, Attorney General Mukasey announced the President's Fiscal Year 2009 budget request for the Department of Justice. The request included \$43.9 million for an Integrated Wireless Network to purchase law enforcement wireless communications. Of the \$43.9 million, \$19 million is for the replacement of outdated communications equipment for the FBI, DEA, ATF, and the Marshall's Service. \$24.9 million is to implement the Integrated Wireless Network in Washington, D.C.</p>

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
High Risk Metropolitan Assistance Project: the 25 Cities Project	<p>This project addresses the following request from the House/Senate CJS Appropriations Subcommittee staff to the DOJ Wireless Management Office (WMO): (1) provide federal law enforcement/ homeland security agencies with basic inter-systems communication for emergency situations; (2) provide an ability to connect with key local authorities (<i>i.e.</i>, fire, police, emergency medical services [EMS]); and (3) address the top 25 metropolitan areas that are likely targets for attack.</p> <p>The WMO has applied a five-phased approach and has worked in tandem with federal, state and local representatives in each city to develop mutually agreeable and unique interoperability solutions tailored to that city/region; where applicable, DOJ has leveraged existing communications infrastructure and ongoing local area interoperability initiatives</p>	Project is designed to enhance the effectiveness and interoperability of law enforcement communications.	In May 2005, the DOJ reported on its efforts to date. This Project remains ongoing.
Community Oriented Policing Service (COPS) Interoperable Communications Technology Program	The COPS Interoperable Communications Technology Program provides funding to help communities develop effective interoperable communications systems for public safety and emergency services providers. Interoperable Communications Technology grants fund projects that explore uses of equipment and technologies to increase interoperability among the law enforcement, fire service, and emergency medical service communities. These projects are the result of thorough planning and demonstrate how new technologies and operating methods can help communities achieve interoperability.	Aids in the research and development of technology for communications interoperability.	<p>In 2006, the COPS Office awarded \$8.8 million to three law enforcement agencies to address the growing need for interoperable communications technology.</p> <p>To date, COPS has awarded more than \$250 million to 65 communities to improve their interoperable communications systems. Most recently, on September 13, 2008, COPS awarded \$159 million in crime fighting technology grants to local communities in twenty-five states and one territory. The grants will be used for integrated voice and data communications networks for the law enforcement agencies.</p>

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
CommTech Program	<p>CommTech is a comprehensive interoperability project targeted at state and local law enforcement agencies.</p> <p>CommTech is developing open architecture standards for voice, data, image, and video communications systems. These standards will help users exchange information among fixed facilities, mobile platforms, and personal devices.</p> <p>CommTech also researches, develops, tests and evaluates technology solutions that facilitate interoperability in a test bed environment. Areas of interest include VoIP; standards-based radios/systems; cognitive radio; software-defined radio; wireless broadband data communications; antenna research; in-building coverage; multi-band radio; and network coverage extension for rural environments.</p>	CommTech facilitates communications interoperability among state and local law enforcement agencies.	<p>Operated through the DOJ's National Institute of Justice (NIJ).</p> <p>The interoperability standards that CommTech ultimately develops will be incorporated into a Strategic Plan that law enforcement agencies can use to achieve interoperability.</p> <p>NIJ funds communications technology research and development through directed solicitations.</p>
U.S. – Canada Initiative to Intercept Counterfeit Network Hardware Manufactured in China	<p>On February 28, 2008, officials from DOJ, FBI, Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP) announced the results of a joint effort with Canada to intercept illegal importation and sale of network hardware from China.</p> <p>The initiative has netted more than 400 seizures of counterfeit Cisco hardware with an estimated value of \$76 million.</p>	Millions of dollars worth of counterfeit communications and computer equipment are smuggled into the U.S. every year.	

U.S. Department of Commerce

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Spectrum Management for the 21st Century: Plan to Implement Recommendations of the President's Spectrum Policy Initiative	<p>In June 2003, President George W. Bush established the Spectrum Policy Initiative to further develop and implement a U.S. spectrum policy for the 21st century that meets the Nation's needs and spurs economic growth. After establishing a task force to consider these issues and seeking comment from the private sector, the Department submitted two reports to the President that reflect the views obtained in June 2004. These reports contained far-reaching recommendations on a wide range of issues. In November, 2004, the President directed the Department to submit a plan to implement the recommendations.</p> <p>In March 2006, NTIA released a report outlining seven projects that would implement the recommendations of the two reports: (1) Improve Stakeholder Participation and Maintain High Qualifications of Spectrum Managers; (2) Reduce International Barriers to U.S. Innovations in Technologies and Services; (3) Modernize Federal Spectrum Management Processes with Advanced Information Technology; (4) Satisfy Public Safety Communications Needs and Ensure Interoperability; (5) Enhance Spectrum Engineering and Analytical Tools; (6) Promote Efficient and Effective Use of Spectrum; and (7) Improve Planning and Promote Use of Market-based Economic Mechanisms in Spectrum Management.</p>	To further develop and implement a U.S. spectrum policy for the 21st century that meets the Nation's needs and spurs economic growth, President George W. Bush established the Spectrum Policy Initiative in June 2003.	<p>NTIA's efforts to complete these projects remains underway. Among other things, NTIA has already established a Spectrum Management Advisory Committee, which is considering a wide variety of issues including how to implement a spectrum sharing test bed. On May 20, 2008, NTIA announced that the following entities would participate in the Spectrum Sharing Innovation Test-Bed: Adapt4 LLC, Adaptrum Inc., BAE Systems, Motorola Inc., Shared Spectrum Company, and Virginia Polytechnic Institute and State University.</p> <p>On March 20, 2008, NTIA released a report on the federal government's use of spectrum. Included in the report were recommendations that the federal government could implement over the next five years. Among them were suggestions to improve interoperability among public safety agencies and to ensure spectrum support for continuity of government operations.</p>

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
A Public Safety Sharing Demonstration	<p>On June 8, 2007, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) released a report, "A Public Safety Sharing Demonstration," analyzing the District of Columbia's Wireless Accelerated Responder Network (WARN). The WARN pilot is a city-wide broadband wireless public safety network. The system uses commercial broadband technology for remote surveillance, chemical and biological detection and several other emergency related services.</p> <p>The report encourages the federal, state and local public safety community to consider utilizing commercial technologies in satisfying broadband interoperable communications among first responders. The report also recommends that agencies consider commercial broadband services, when feasible.</p>	Intended to improve management of the nation's airwaves, by addressing planning, usage and sharing of spectrum, and the feasibility of using commercial services to meet the increasingly complex wireless broadband needs of public safety.	<p>The report is available on NTIA's website at http://www.ntia.doc.gov/reports/NTIAWARNRreport.pdf.</p> <p>The report's recommendations may be used in the further development and implementation of public safety communications and spectrum policies.</p>

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Public Safety Interoperable Communications Grant Program	NTIA and DHS signed a Memorandum of Understanding on Friday, February 16, 2007, to implement the Public Safety Interoperable Communications Grant Program to help state, local and federal first responders better communicate during a natural or man-made disaster.	The grant program, which covers public safety agencies in all 50 states, the District of Columbia, Puerto Rico and four U.S. territories, will assist public safety agencies in the acquisition, deployment, or training for the use of interoperable communications systems that can utilize reallocated public safety spectrum in the 700 MHz band for radio communication.	On July 18, 2007, U.S. Commerce Secretary Carlos M. Gutierrez and U.S. Homeland Security (DHS) Secretary Michael Chertoff announced the availability of \$968 million in Public Safety Interoperable Communications Grants to help state and local first responders improve public safety communications and coordination during a natural or man-made disaster for all 50 states, the District of Columbia, and the U.S. territories. Public safety organizations interested in PSIC funding could seek funding through their State Administrative Agency. The deadline for submission of each State and Territory's Investment Justification was December 3, 2007.



U.S. Department of Agriculture

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Rural Information Center (RIC)	<p>The Rural Information Center provides information and referral services to local, tribal, state, and federal government officials; as well as community organizations, rural electric and telephone cooperatives, libraries, businesses, and citizens working to maintain the vitality of America's rural areas.</p> <p>RIC also provides resources for communications interoperability and emergency preparedness.</p>	RIC provides resources to local officials to improve emergency communications in rural areas.	RIC has released publications such as Rural Homeland Security Resources for Local Officials and Rural Fire Department Resources for Local Officials, which provide lists of planning and training resources for local officials as well as information on funding and program assistance.
Rural Broadband Loans	<p>On March 25, 2008, USDA Rural Development Undersecretary Thomas Dorr announced a \$267 million loan to a Colorado company to provide broadband to 518 rural communities in 17 states.</p> <p>The project will give more than 6 million people access to portable, affordable broadband.</p>	Access to broadband in these communities will improve communications for first responders, law enforcement, and health providers.	This loan was issued under the Rural Development Broadband Loan and Loan Guarantee program which has awarded \$1.6 billion in loans.
Broadband Community Connect Grants	<p>On October 4, 2007, Acting Secretary of Agriculture Chuck Conner announced the award of \$10.3 million in broadband community connect grants.</p> <p>In a number of the communities served by these grants, funds will support broadband and computers that offer public safety messages and telemedicine services.</p>	Grant funds will go toward purchasing computers and communications equipment in rural communities.	



U.S. Department of Health and Human Services

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
The Emergency Preparedness Resource Inventory (EPRI)	<p>EPRI is a web-based tool allowing local or regional planners to assemble customized inventories of critical resources that would be useful in responding to a bioterrorist attack, including health care and emergency resources.</p> <p>The tool uses the Internet so communities can assess their regional supply of critical resources, prepare for incident response, estimate gaps, support future resource investment decisions, and help first responders figure out where emergency equipment and medicines are located, how much is available, and whom to contact to obtain those resources.</p>	This tool utilizes the Internet to disseminate emergency information to local and regional governments.	Released by HHS' Agency for Healthcare Research and Quality in May 2005.
New Emergency Information Center Model	This operations model for emergency call centers is designed to help public health agencies and other first responders prepare to provide accurate, timely information during a health emergency. The model is also designed to help public health departments, state and local officials and others gear up quickly to answer calls from the public and health care providers if an emergency arises.	The model offers guidance to organizations on the requirements, specifications and resources needed to develop a public health emergency contact center that is highly integrated with public health agencies and that can reduce the likelihood of hospitals and health systems being overwhelmed with calls and requests for information.	<p>Released by HHS' Agency for Healthcare Research and Quality in March 2005. The model is available for download at the HHS Agency for Healthcare Research and Quality website.</p> <p>A goal of the model is to develop the capacity to handle 1,000 calls per hour from health care providers or members of the public in addition to delivering regular services.</p>

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Public Health Emergency Grants	<p>On June 3, 2008, HHS Secretary Mike Leavitt announced that HHS made available nearly \$1.1 million to hospitals, public health agencies, and other organizations to respond to public health and medical emergencies.</p> <p>Of these funds, \$398 million will come from the Hospital Preparedness Program for use in implementing interoperable communication systems and other emergency response measures in hospitals.</p>	Funds will support adding interoperable communications systems to hospital and public health agencies.	
Health Care Summit on Emergency Communications	On November 1, 2007, the FCC and HHS held a joint Health Care Summit on Emergency Communications: Preparedness, Response and Recovery.	The Summit focused on hospital emergency communications plans and preparedness efforts, including the use of alternative technologies to bolster response capabilities.	